20th May 2022

Cyber Security And The High-Risk Environment Of Electronic Products

History of Major Cyber Crimes

Cybercrime is such a fast-paced, constantly evolving sector that no cybersecurity program can be perfect. When it comes to partnering with the people responsible for managing your IP on a daily basis, it is necessary to be cyber-aware to prevent breaches or minimize damage when they occur (refer to image at the end of this article to see a snapshot of how security threats have evolved over the years).

The Internet has made information easily accessible to a wider audience. Information and ideas can be exchanged more quickly and easily than ever before. This is a great advancement for humanity. Now we must ensure that only those we want have access to this data. That is the essence of cybersecurity.

"the state of being safe from electronic crime and the measures taken to achieve this".

Our role as contract manufacturers includes collaborating with our customers around the globe to deliver a product or service. By combining our expertise with theirs, we can create something truly unique. Innovation demands the protection of ideas so we can make sure we, and our customers, stay competitive. Protecting data is the responsibility of every stakeholder, whether they are involved with a medical device, military hardware, commercial product, or product component.

This article has been developed for electronic product innovators working with sensitive information relating to their IP who need to, at some point or another, partner with organizations outside of their own to manage their product life cycle effectively.

Cyber Security Framework

A cyber security framework outlines guidelines, standards, and best practices for managing cybersecurity risks. A product innovator should consider the framework that will surround and guide their IP and product security when they partner with an electronics contract manufacturer. Identifying and embracing security aspects such as the latest technologies and methods, third-party providers, data security, geographic security, firewalls, and other layers of protection should be a priority for contract manufacturers.

For the Aviation, Space and Defense (AS&D) industry to meet the AS9100 standard, the standard should be held by the contract manufacturer. As an added layer of security, DISP (Defence Industry Security Program) accreditation is available in Australia. In addition to other protections, these together provide a strong level of cyber security.

If you're familiar with the range of different quality system standards, you'll notice that one word connects them all. This is "risk." What are the risks that can stop your business from achieving its best results? Any project begins with a system review, and you should look for risks that could compromise your objectives, as well as the systems of your partners. In a business, people and infrastructure are the two most important areas of risk.

Cyber security can seem complicated and overwhelming, but there is a lot of help and advice available online. Legislative authorities, advisory groups, and third-party providers often assist in this area.

An excellent resource for Australian product innovators is the Australian Cyber Security Centre.

The Cyber Security and Infrastructure Security Agency will guide you through a variety of resources relating to cyber security if you are a US product innovator.

Using a cyber security assessment tool can help you identify your strengths and areas for improvement:
US Cyber Security Tool
Australian Cyber Security Tool

People and Infrastructure
If you are serious about cyber security, make sure that you focus first on your people and infrastructure.

Infrastructure (Hardware and Software Components)
The Essential 8 is a set of fundamental cybersecurity threat mitigation strategies. Integrating the Essential 8 into your cyber security protocol will make it harder for adversaries to compromise your systems.

The Essential 8 includes:
1. Application control
2. Patch applications
3. Configure Microsoft Office macro settings
4. User application hardening
5. Restrict administrative privileges
6. Patch operating systems
7. Multi-factor authentication
8. Regular backups

People
The greatest asset of any organization is its people. On the other hand, people can also pose a significant risk to the system as a whole. Bringing everyone along on this journey is essential, leveraging their knowledge and providing training and awareness of cyber security.

Several methods can be used to engage your employees. The Cybersecurity & Infrastructure Security Agency (CISA) in the US provides game apps to aid in learning the security concepts.

Our employees receive security awareness training every month.

Cyber security breaches are explained in our training, as well as best practices for dealing with them. We cover topics such as:
- Phishing and identity theft
- Macro malware
- Pad passwords and USBs
- 2FA security
- Ransomware
- Home and VPN security
- Social engineering
- Physical security
- SMS security

It is important that your contract manufacturer views your relationship as a partnership, developing cyber security protocols to ensure your success. As certain cyber security areas are specialized, your contract manufacturer should avoid trying to 'do it all' and instead engage third parties that can offer direct cyber security experts such as IT and managed services.

As part of regular training, IT and managed service providers should also offer people training and testing in the following areas:

1. Phishing Campaign: Random emails to check compliance
2. Password Audit: Verifying the robustness of users' passwords checked annually.
3. Penetration Testing: How easy is it to break down the hardware & software barriers checked.
4. Vulnerability Scanning: Making sure our patching is up to date and looking for other weaknesses.
5. Performance Review: We have regular meetings to discuss the health of our systems and look for areas to improve both in the hardware/software realm and to improve the knowledge of our employees.

External Interactions

We have a proprietary numbering scheme for our internal parts and for interactions with our suppliers.

Clients' data is uploaded in a unique client code for cross-referencing and communication, which is an additional layer of security above normal CM interactions and part of the protection of our client's IP.

Conclusion

So, what about the future?

Other than a few "Ethical Hackers," the most common threat is money-making. Going forward, ransomware will be the most popular and most likely to grow:

"ACSC In 2021, cybersecurity authorities in the United States, Australia, and the United Kingdom observed an increase in sophisticated, high-impact ransomware incidents against critical infrastructure organizations globally".

It is crucial you do not allow the hackers into your system. Internet connections and keyboards are the two primary entry points into a system. Get yourself a partner you can trust, do a comprehensive risk assessment, and educate yourself and your employees.

Please visit these links if you require additional assistance in cyber security or please contact us if you want to learn more about how our company ensures the security of IP belonging to our customers across a variety of countries:

https://civilservice.blog.gov.uk/2015/10/06/cyber-security-is-everyones-responsibility/
https://www.stonegroup.co.uk/insights/what-makes-up-an-it-infrastructure/
https://www.ncsc.gov.uk/information/infographics-ncsc#section_3
https://www.ncsc.gov.uk/